SIEMENS

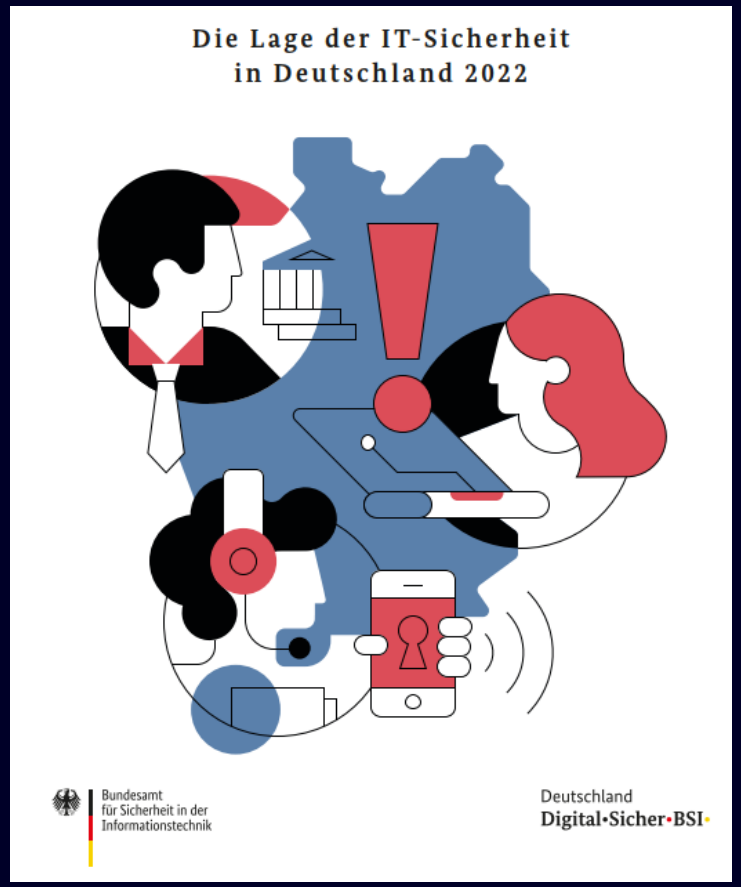
Anomalieerkennung & Cybersicherheit

Systeme zur Angriffserkennung in der Energieautomatisierung

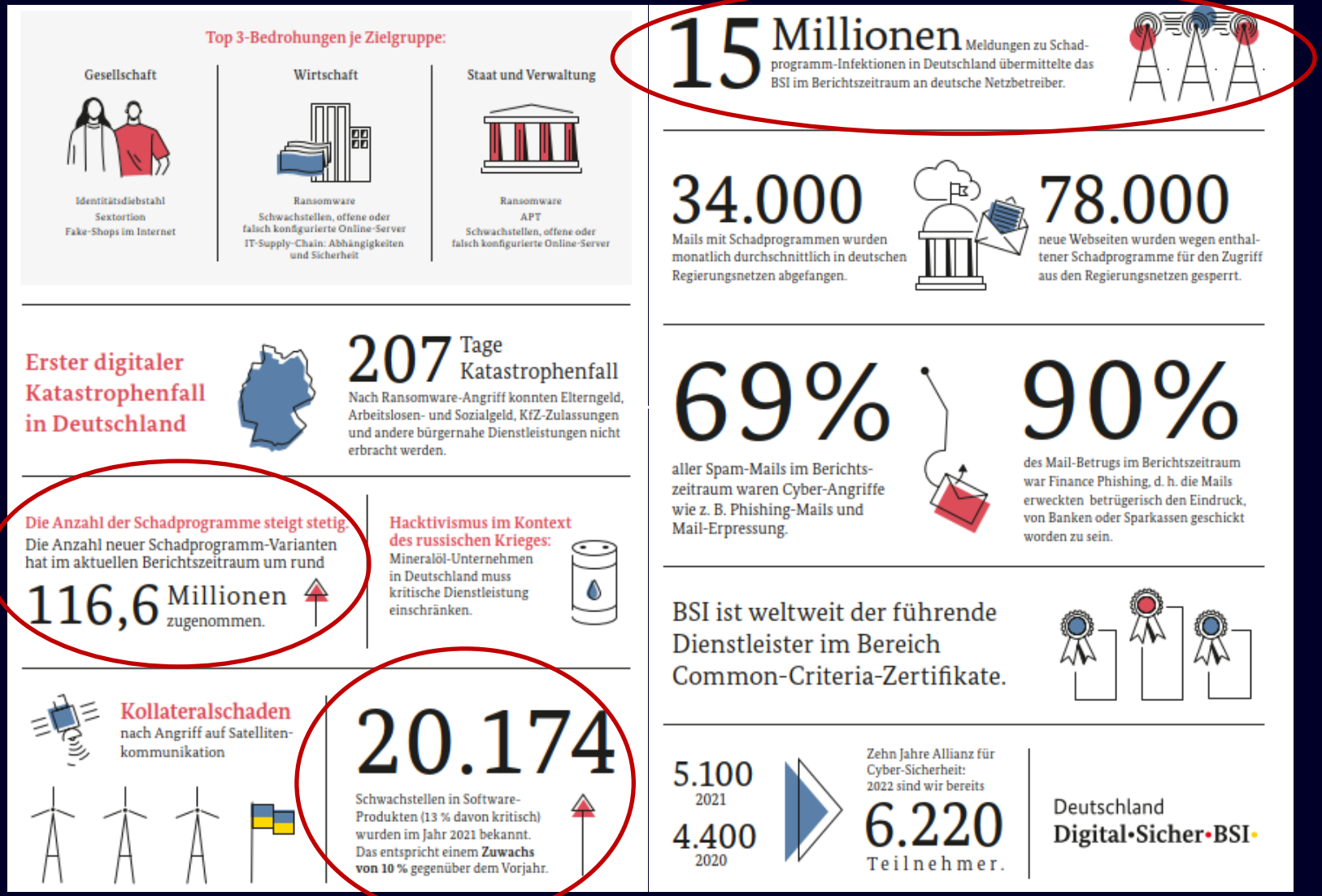
(Anforderungen aus dem IT-Sicherheitsgesetz 2.0)

Lage der IT-Sicherheit in Deutschland

BSI-Lagebericht 2022 (Auszug)



Quelle: BSI Lagebericht 2022 https://www.bsi.bund.de



SIEMENS

Gesetzliche und Regulatorische Anforderungen

…im Sektor Energie

Bundesministerium des Innern, für Bau und Heimat

PRESSEMITTEILUNG · 23.04.2021

Bundestag verabschiedet IT-Sicherheitsgesetz 2.0

Seehofer: "Ein Meilenstein für die Cybersicherheit in Deutschlan

Der Bundestag hat heute den von Bundesinnenminister Horst Seehofer vorgelegten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherh verabschiedet.

Bundesinnenminister Horst Seehofer: *"Das IT-Sicherheitsgesetz 2.0 ist ein Zukunftsgese riesen Sprung nach vorn und ein echter Meilenstein für unsere Cybersicherheit. Das Projek beeindruckender Weise, dass Digitalisierung und Cybersicherheit im Bundesinnenminister haben."*

Das IT-Sicherheitsgesetzes 2.0 enthält unter anderem folgende Neuerungen:

- **BSI wird als Deutschlands zentrale Cybersicherheitsbehörde gestärkt:** …
- **Cybersicherheit in den Mobilfunknetzen:** …
- **Stärkung des Verbraucherschutzes:** …
- **Mehr Sicherheit für Unternehmen:** Betreiber Kritischer Infrastrukturen sowie kün Unternehmen im besonderen öffentlichen Interesse (z.B. Rüstungshersteller oder besonders großer volkswirtschaftlicher Bedeutung) müssen künftig bestimmte IT-S umsetzen und werden in den vertrauensvollen Informationsaustausch mit dem BSI einbezogen.

Bundesministerium für Wirtschaft und Klimaschutz

Technologien · Recht und Politik · Forschung

Sie sind hier: » Startseite » Recht und Politik » Weitere Gesetze und Verordnungen

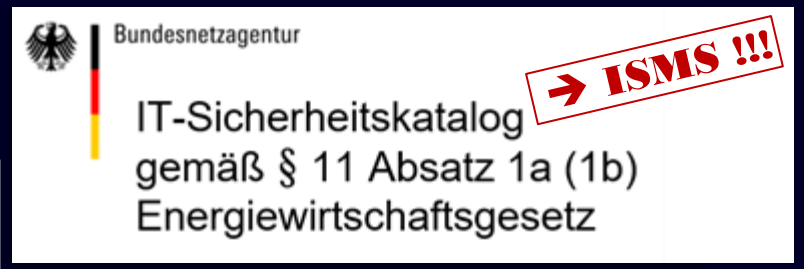
Energiewirtschaftsgesetz (EnWG)

Zweck des Gesetzes ist eine möglichst sichere, preisgünstige, verbraucherfreundliche, effiziente und umweltverträgliche leitungsgebundene Versorgung der Allgemeinheit mit Elektrizität und Gas, die zunehmend auf erneuerbare Energien beruht.

Das EnWG gewährleistet im Rahmen seiner Bestimmungen unter anderem eine fortlaufend transparente und koordinierte Netzausbauplanung für das deutsche Höchstspannungsnetz. Die Ermittlung des Netzausbaubedarfs verläuft dabei in einem mehrstufigen Verfahren.

Weiterführende Informationen

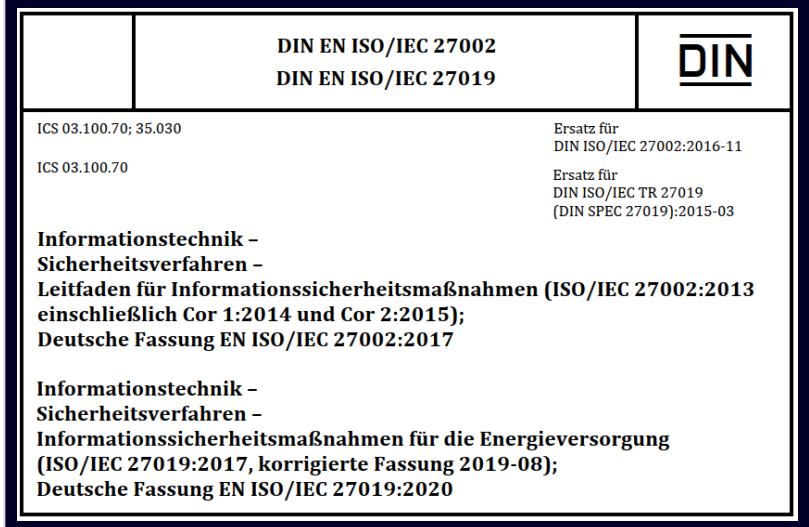
- Energiewirtschaftsgesetz (EnWG)
- BMWi.de - Stromnetze und Netzausbau: Regulierung und Rahmenbedingungen



Bundesnetzagentur

→ ISMS !!!

IT-Sicherheitskatalog gemäß § 11 Absatz 1a (1b) Energiewirtschaftsgesetz



DIN EN ISO/IEC 27002
DIN EN ISO/IEC 27019

DIN

ICS 03.100.70; 35.030

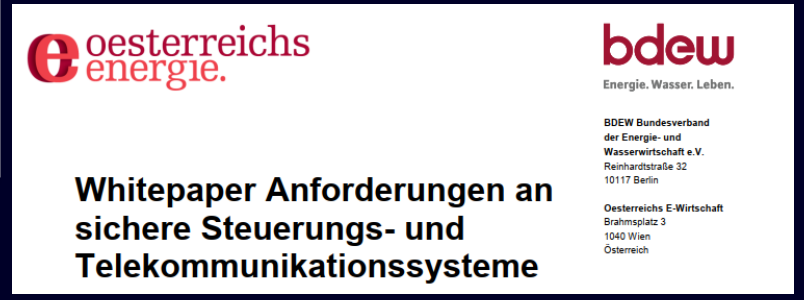
ICS 03.100.70

Ersatz für
DIN ISO/IEC 27002:2016-11

Ersatz für
DIN ISO/IEC TR 27019
(DIN SPEC 27019):2015-03

Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017

Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08); Deutsche Fassung EN ISO/IEC 27019:2020



oesterreichs energie.

bdew
Energie. Wasser. Leben.

Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Oesterreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

SIEMENS

BSI Dokument: OH-SzA

Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

BSI veröffentlicht Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

BSI veröffentlicht Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Kritische Infrastrukturen (KRITIS) > KRITIS-FAQ > FAQ Systeme zur Angriffserkennung (§ 8a Absatz 1a BSIG)

Das Energieversorgungsnetz erreicht nicht den Schwellenwert aus der BSI-Kritisverordnung. Welche Regelungen gelten?

Gemäß § 11 Absatz 1d EnWG sind Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, dazu verpflichtet, Ihre Anlagen beim BSI zu registrieren und eine Kontaktstelle zu benennen. Auf Basis dieser Registrierung müssen die Betreiber dem BSI IT-Störungen melden (vgl. § 11 Absatz 1c EnWG) und erstmalig zum 1. Mai 2023 nachweisen, dass Systeme zur Angriffserkennung eingesetzt werden (vgl. § 11 Absatz 1e EnWG). Diese Verpflichtungen betreffen alle Betreiber von Energieversorgungsnetzen, unabhängig von den in der BSI-Kritisverordnung genannten Schwellenwerten.

https://www.bsi.bund.de/.../faq-systeme-angriffserkennung_node.html

Betreiber von Energieanlagen und Energieversorgungsnetzen vor. Das Dokument eignet sich zudem als Grundlage für die Fortentwicklung der Branchenspezifischen Sicherheitsstandards (B3S) im Zuge der Integration der SzA.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html

SIEMENS

Unterschiedliche Möglichkeiten

… zur Angriffserkennung

IPS
Intrusion Prevention System

Virenscanner
Malware Detection

XDR
Extended Detection & Response

SOC
Security Operation Center

MDR
Managed Detection and Response

EDR
Endpoint Detection & Response

SIEM
Security Information Event Management

IDS
Intrusion Detection System

LogServer
Syslog-Protokoll

Xyz
……

Als Anwender stellt man sich die Frage:

Welche dieser Systeme sind für den OT-Bereich sinnvoll, angemessen und notwendig?

SIEMENS

BSI OH-SzA

Anforderungen: Protokollierung, Detektion

Inhalt

Umsetzung der Protokollierung

Als Mindestanforderung für die Protokollierung MÜSSEN alle Basisanforderungen von OPS.1.1.5 *Protokollierung* und die folgenden Anforderungen erfüllt werden:

Aufbau zentralisierter Protokollierungsinfrastrukturen:

Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen[5] Stellen gespeichert werden. Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst geringgehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann.

Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein. Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.

Bereitstellung von Protokoll- und Protokollierungsdaten für die Auswertung:

Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.

...NN den

Umsetzung der Detektion

Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 *Detektion von sicherheitsrelevanten Ereignissen* und die folgenden Anforderungen erfüllt werden:

Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten:

Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden. Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist. Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen.

Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind.

⋮

Für die Detektion von sicherheitsrelevanten Ereignissen MÜSSEN genügend personelle Ressourcen bereitgestellt werden.

Einsatz zusätzlicher Detektionssysteme:

Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden. Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

SIEMENS

BSI OH-SzA

Anforderung: Reaktion

Inhalt

Reaktion

Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 *Behandlung von Sicherheitsvorfällen* erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.

Es SOLLTEN zudem die Standardanforderungen aus DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.

…MUSS die folgende Anforderung erfüllt werden:

Automatische Reaktion auf sicherheitsrelevante Ereignisse:

Bei einem sicherheitsrelevanten Ereignis **MÜSSEN** die eingesetzten Detektionssysteme das Ereignis automatisch melden…

Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird.

Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom MUSS schlüssig begründet sein.

Die zur Angriffserkennung eingesetzten Systeme **SOLLTEN** automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende sicherheitsrelevante Ereignis eindeutig qualifizierbar ist.

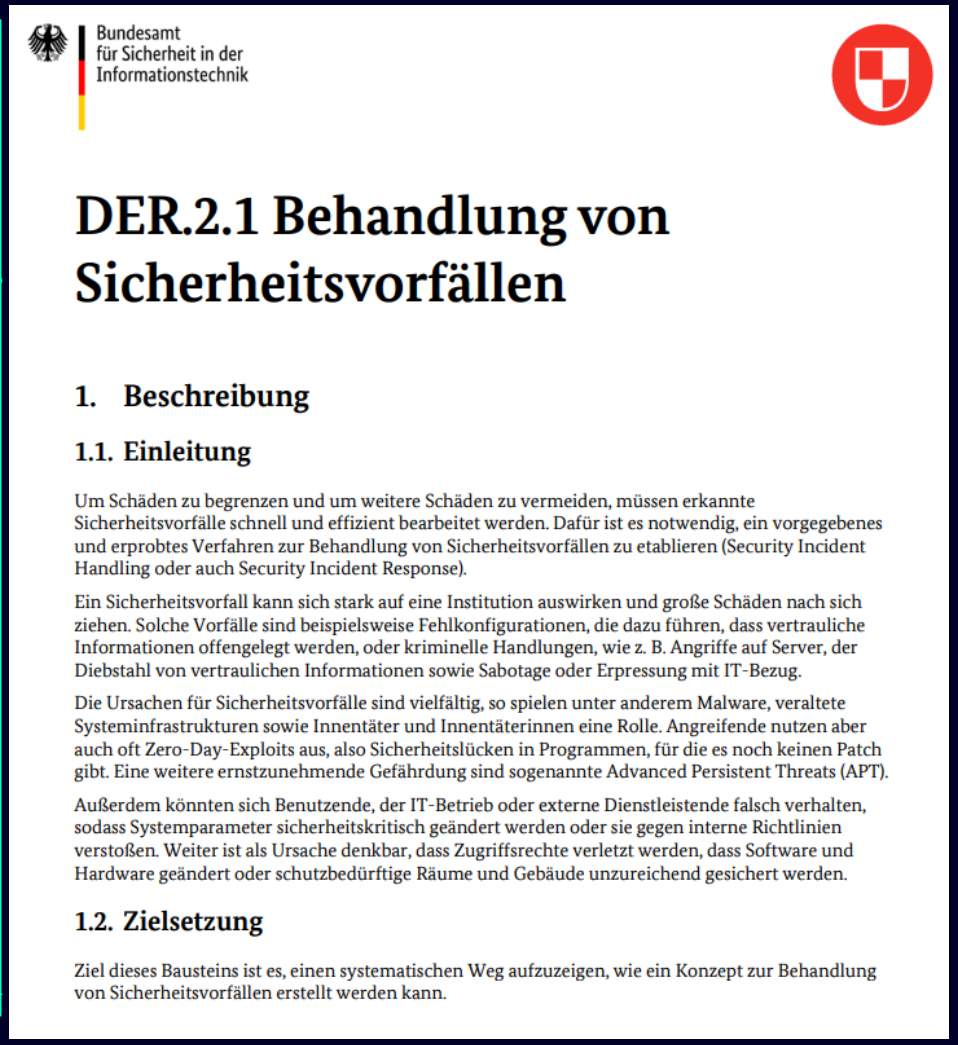
Dabei **MUSS** gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.

SIEMENS

BSI OH-SzA

Anforderung Reaktion ⇨ IT-Grundschutz Baustein “DER.1”

https://www.bsi.bund.de/.../05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen...



Bundesamt
für Sicherheit in der
Informationstechnik

DER.2.1 Behandlung von Sicherheitsvorfällen

1. Beschreibung

1.1. Einleitung

Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren (Security Incident Handling oder auch Security Incident Response).

Ein Sicherheitsvorfall kann sich stark auf eine Institution auswirken und große Schäden nach sich ziehen. Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden, oder kriminelle Handlungen, wie z. B. Angriffe auf Server, der Diebstahl von vertraulichen Informationen sowie Sabotage oder Erpressung mit IT-Bezug.

Die Ursachen für Sicherheitsvorfälle sind vielfältig, so spielen unter anderem Malware, veraltete Systeminfrastrukturen sowie Innentäter und Innentäterinnen eine Rolle. Angreifende nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, für die es noch keinen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT).

Außerdem könnten sich Benutzende, der IT-Betrieb oder externe Dienstleistende falsch verhalten, sodass Systemparameter sicherheitskritisch geändert werden oder sie gegen interne Richtlinien verstoßen. Weiter ist als Ursache denkbar, dass Zugriffsrechte verletzt werden, dass Software und Hardware geändert oder schutzbedürftige Räume und Gebäude unzureichend gesichert werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, einen systematischen Weg aufzuzeigen, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt werden kann.

- **Anforderungen**
  Beispiele:
  - Definition eines Sicherheitsvorfalls (B)
  - Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen (B)
  - Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (B)
  - Behebung von Sicherheitsvorfällen (B)
  - Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen (B)
  - Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen (S)
  - Eindämmen der Auswirkung von Sicherheitsvorfällen (S)
  - Eskalationsstrategie für Sicherheitsvorfälle (S)
  - Dokumentation der Behebung von Sicherheitsvorfällen (S)

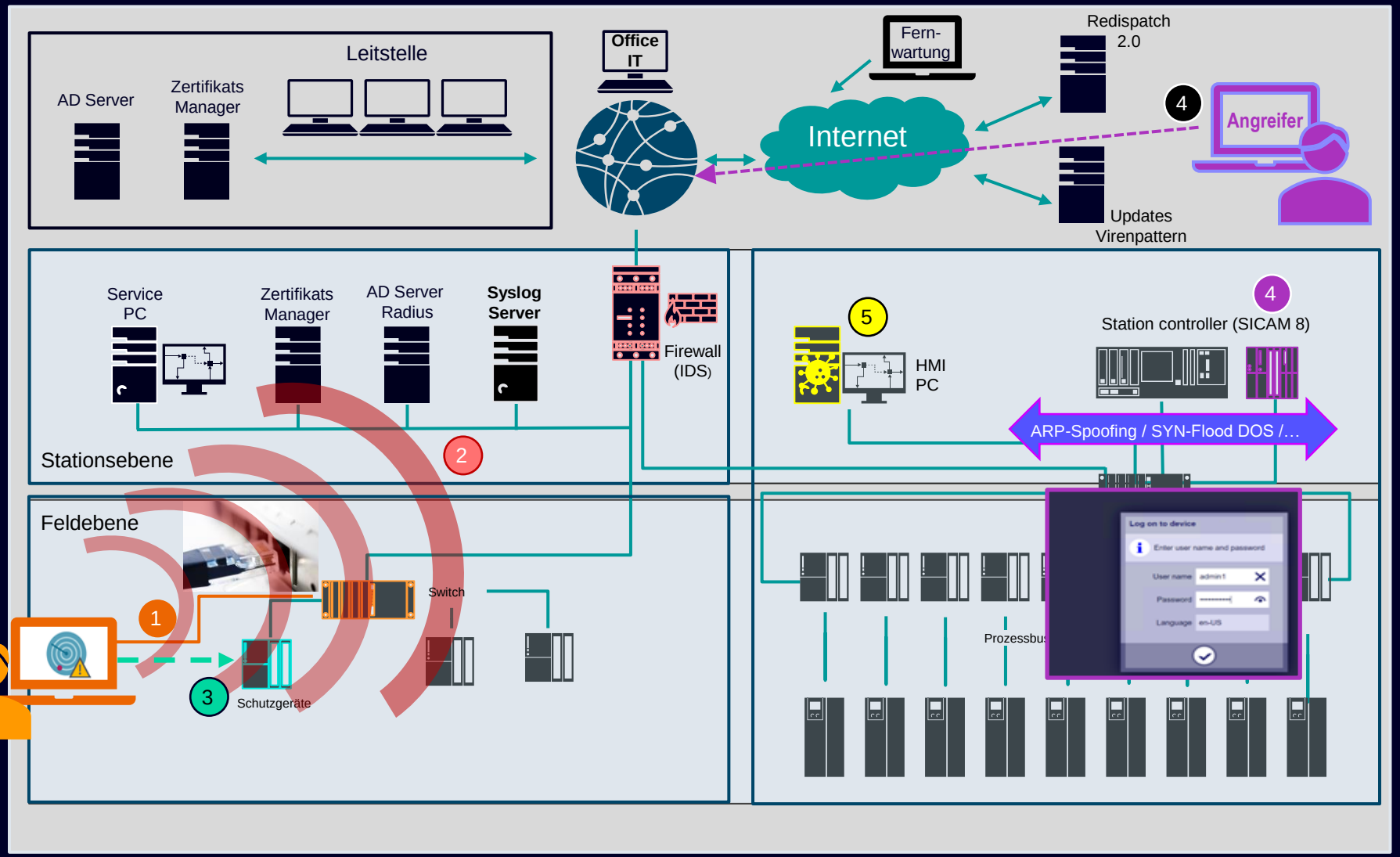
  (B) = Basis-Anforderung | (S) = Standard-Anforderung

BSI: IT Grundschutz-Bausteine
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

SIEMENS

Vielfältige Bedrohungen

Beispiele möglicher Angriffsversuche



1. unerlaubtes Anschließen an einen Switch
2. Netzwerk-/ Portscan (Intrusion Detection System)
3. lokaler Engineeringzugriff auf ein Endgerät
4. Anmeldeversuch an einem Endgerät via Web Interface
5. Schadsoftware auf einem Windows-Rechner (Virenscanner/EDR)
6. Angriffe auf (OT-)Endgeräte z.B.:
   - ARP-Spoofing oder
   - SYN-Flood (DoS) Angriff
   - dysfunktionaleTelegramme

SIEMENS

BDEW Whitepaper und ISO/IEC 27002

(zentrales) Logging

oesterreichs energie.

bdew
Energie. Wasser. Leben

4.5.6 Logging

Sicherheits-anforderungen	ISO/IEC 27002:2013 / 27019:2017 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3
dezentrale(s) Erfassung (Logging)	a) Das Gesamtsystem muss über eine einheitliche Systemzeit verfügen und die Möglichkeit zur Synchronisation dieser Systemzeit mit einer externen, gesicherten Zeitquelle bieten.
	b) Das System muss Benutzeraktionen sowie sicherheitsrelevante Aktionen, Vorkommnisse und Fehler in einem zur nachträglichen und zentralen Auswertung geeignetem Format protokollieren. Es werden Datum und Uhrzeit, involvierte Benutzer und Systeme sowie das Ereignis und Ergebnis für einen konfigurierbaren Mindestzeitraum aufgezeichnet.
zentrales Logging (⇨ SysLog Protokoll)	c) Die zentrale Speicherung der Logdateien erfolgt an einem frei konfigurierbaren Ort. Ein Mechanismus zur automatisierten Übertragung des Logfiles auf zentrale Komponenten muss zur Verfügung stehen.
	d) Das Logfile muss gegen spätere Modifikation geschützt sein.
Alarm-Management (⇨ Auswertung der srel. Ereignisse)	e) Bei Überlauf des Logfiles werden die älteren Einträge überschrieben, das System muss bei knapp werdendem Logging-Speicherplatz warnen.
	f) Es muss möglich sein, sicherheitsrelevante Meldungen in ein vorhandenes Alarm-Management aufzunehmen.

DIN EN ISO/IEC 27002 — DIN

ICS 03.100.70; 35.030

Ersatz für
DIN ISO/IEC 27002:2016-11

**Informationstechnik –
Sicherheitsverfahren –
Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015);
Deutsche Fassung EN ISO/IEC 27002:2017**

12.4 Protokollierung und Überwachung

Ziel: Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.

12.4.1 Ereignisprotokollierung

Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, sollten erzeugt aufbewahrt und regelmäßig überprüft werden.

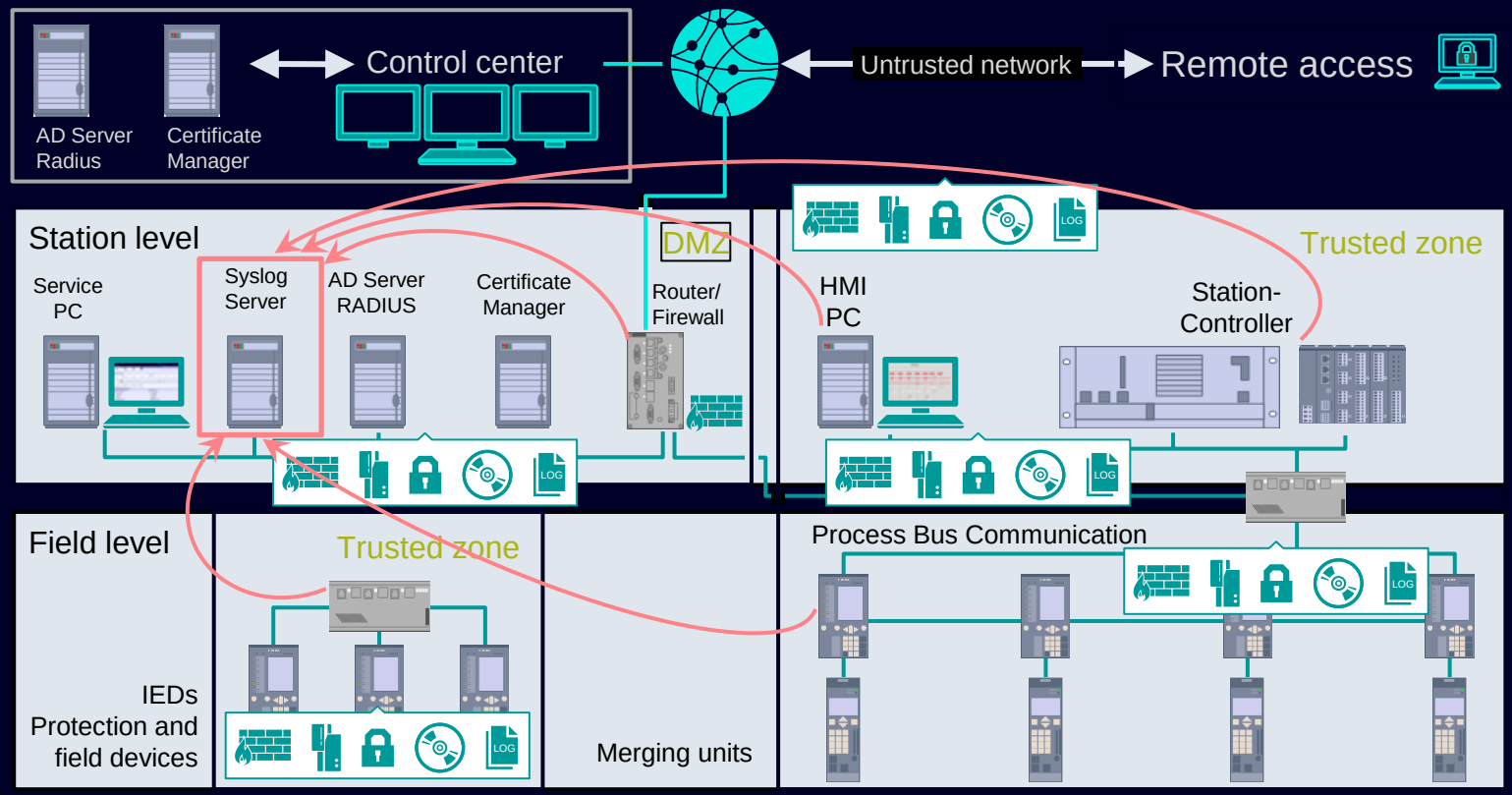
b) Systemaktivitäten;
c) Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. Anmeldung und Abmeldung;
d) Geräteidentität oder -standort (falls möglich) und Systembezeichnung;
e) Aufzeichnung erfolgreicher und abgelehnter Systemzugriffsversuche;
f) Aufzeichnung erfolgreicher und abgelehnter Versuche, auf Daten oder andere Ressourcen zuzugreifen;
g) Änderungen der Systemkonfiguration;
h) Nutzung von Privilegien;
i) Nutzung von Dienstprogrammen und Anwendungen;
j) Dateien, auf die zugegriffen wurde, und Art des Zugriffs;
k) Netzwerkadressen und Protokolle;

Die Ereignisprotokollierung bildet den Grundstein für automatisierte Überwachungssysteme, die in der Lage sind, konsolidierte Berichte und Warnungen zur Systemsicherheit zu erzeugen.

SIEMENS

Security Logging

⇨ Protokollierung in einem zentralen Syslog-Server



Cyber security measures

- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, Backup and restore
- Malware protection
- Data protection, data integrity and system architecture
- Secure remote access

- **SYSLOG-Protokoll**

  Um securityrelevante Informationen zu sammeln und an einen zentralen Server zu übertragen kommt meist das standardisierte Syslog-Protokoll zum Einsatz.

  Ein zentraler Syslog-Server sammelt dabei die Syslog-Meldungen der unterlagerten (End-) Geräte ein.

SIEMENS

Dezentrales Logging von OT-Geräten

Beispiel: Syslog-Ereignisse SIPROTEC 5 Schutzgerät

8.3.2 Syslog-Ereignisse SIPROTEC 5

Schweregrad Ereignis

Die folgende Tabelle zeigt das syslog mit Schweregrad ***Ereignis***.

Ereignis	Zusätzliche Angaben	
User caused a control operation %A1%. (Benutzer hat Steuerungshandlung %A1% ausgelöst.) Zusätzliche Angaben: %A2%	%A1%	Der Typ der ausgeführten Steuerungshandlung, zum Beispiel Deaktivierung des Leistungsschalters
	%A2%	Zusätzliche Angaben zur Steuerungshandlung, zum Beispiel <FG.FN.FB.Signalname des Leistungsschalters gemäß DIGSI 5-Betriebsmeldepuffer>

Schweregrad Alarm

Die folgende Tabelle zeigt das syslog mit Schweregrad ***Alarm***.

Alarm	Zusätzliche Angaben	
While logging on to user account %A1% (%A2%-managed account) from %A3%, 3 incorrect password entries in succession were attempted. (Bei der Anmeldung an Benutzerkonto %A1% (%A2%-verwaltetes Konto) von %A3% wurde das Passwort 3-mal hintereinander falsch eingegeben.)	%A1%	Konto-ID
	%A2%	Kontotypen: • Beim produktverwalteten (lokalen) Benutzerkonto ist der Kontotyp der Produktname. • Beim RADIUS-Benutzer ist der Kontotyp ***RADIUS***.
	%A3%	%A3% kann Folgendes sein: • Der benutzerbezogene Name des Produkts, bei dem Anmeldeversuche erkannt wurden • Wenn ein Fernbedienplatz verwendet wird, ist %A3% die IP-Adresse des Fernbedienplatzes. • Bedieneinheit des Gerätes

SIPROTEC 5, Sicherheit, Handbuch
C53000-H5000-C081-4, Ausgabe 11.2020

Beispiel einer Syslog-Datei:

<105>1 2019-05-07T13:13:54.123+01:00 172.16.21.223 Mainboard - Siemens-Grid-Security - 'L3_TX101_7SJ82_2 Three incorrect password entries in succession were attempted while logging in to user account 'OPERATOR' ('RADIUS'-managed account) from 'HMI'.
<105>1 2019-05-07T13:13:48.246+01:00 172.16.21.222 Mainboard - Siemens-Grid-Security - 'L2_TX102_6MD85': Repeated attempt to log in to user account 'OPERATOR' ('RADIUS'-managed account) from 'HMI'.
<14>Feb 11 17:52:46 192.168.21.13 Microsoft-Windows-Security-Auditing[0x11dc]: {"EventTime":"2020-02-11T17:52:46.371858+01:00","Hostname":"SS02-HMIS01.scm.local","Keywords":"9232379236109516800","EventType":"AUDIT_SUCCESS","SeverityValue":2,"Severity":"INFO","EventID":4670,"SourceName":"Microsoft-Windows-Security-Auditing","ProviderGuid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","Version":0,"TaskValue":13570,"OpcodeValue":0,"RecordNumber":11316845,"ExecutionProcessID":4,"ExecutionThreadID":3312,"Channel":"Security","Message":"Permissions on an object were changed.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSS02-HMIS01$\r\n\tAccount Domain:\t\tSCM\r\n\tLogon ID:\t\t0x3E7\r\n\r\nObject:\r\n\tObject Server:\tSecurity\r\n\tObject Type:\tToken\r\n\tObject

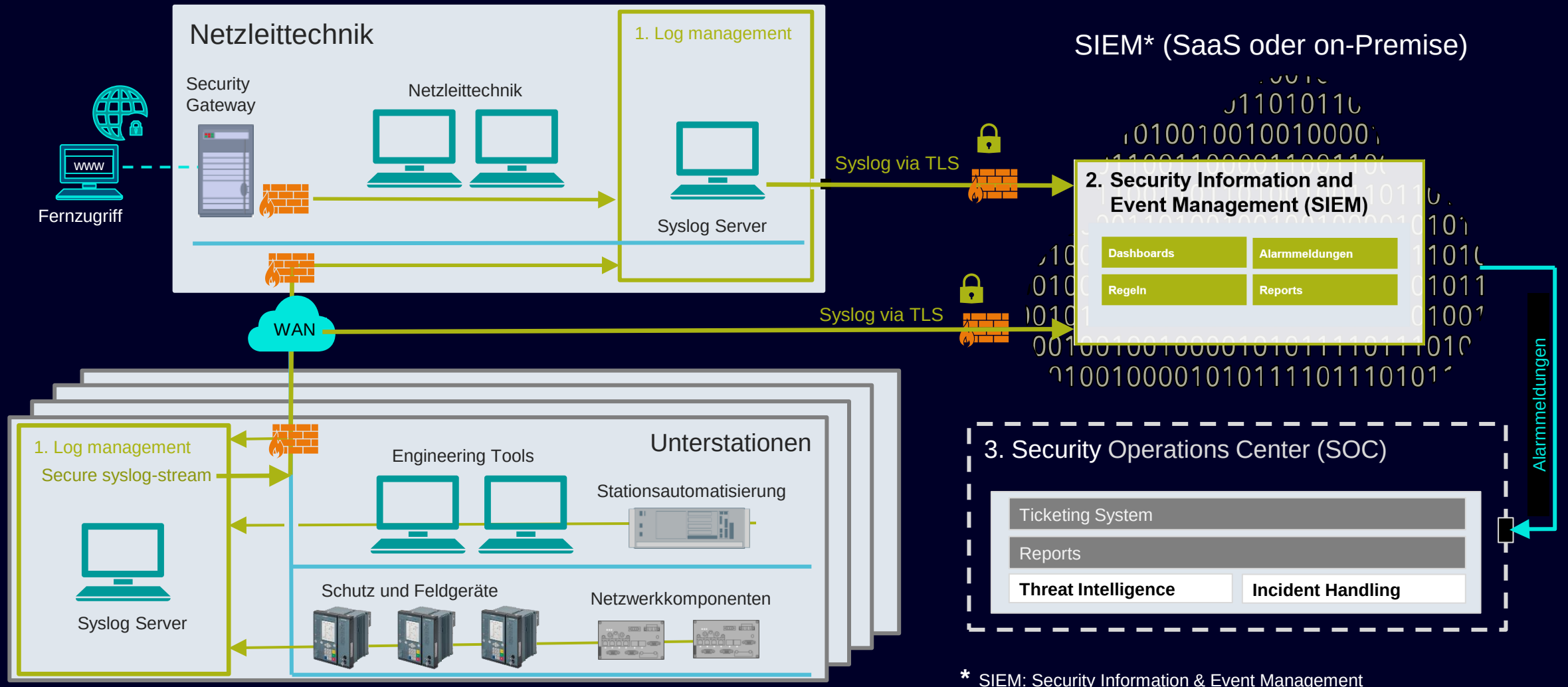
Herausforderungen:

- **Sammelt ein Syslog-Server die Syslog-Meldungen aller angeschlossenen Komponenten, wachsen diese Log-Files sehr schnell an.**
- **Diese Meldungen sind für einen Menschen eher schwer lesbar!**
- **Das führt dazu, dass es sehr schwer und zudem ziemlich unübersichtlich ist das regelmäßig („händisch“) zu überprüfen und die wichtigen von den unwichtigen Meldungen zu trennen!**

SIEMENS

Security Logging / Monitoring

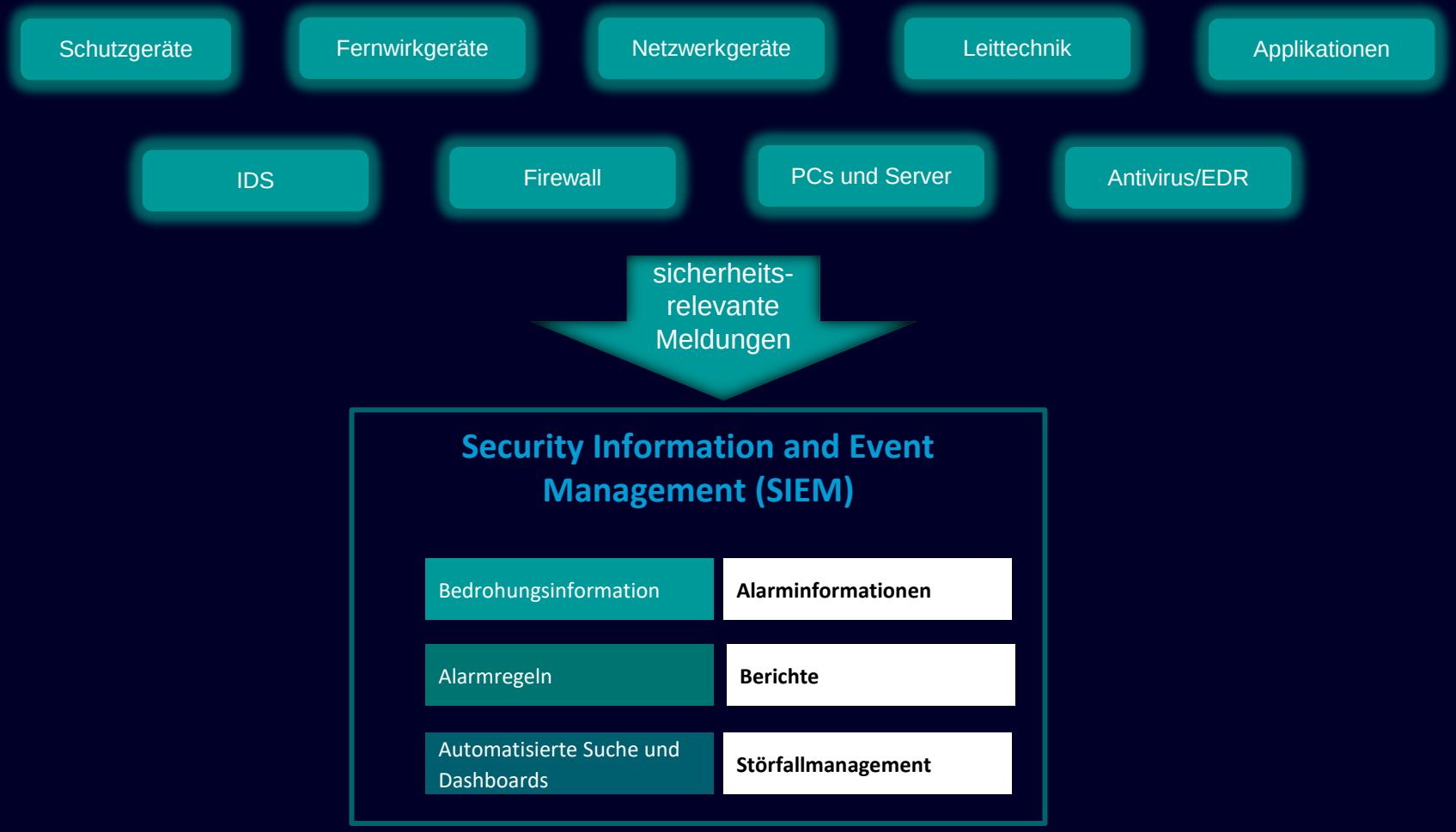
⇨ automatische Auswertung/Alarmierung mittels eines (OT-)SIEM Systems



* SIEM: Security Information & Event Management

SIEMENS

OT-SIEM ➔ System zur Angriffserkennung



dezentrales Logging von (securityrelevanten) Ereignissen (Syslog Protokoll)

zentrales Sammeln von Logging-Informationen (Syslog Server)

Auswerten und Bewerten securityrelevanter Informationen ➔ Alarmierung (SIEM-System)

SIEMENS

Drei Beispiel-Use-Cases aus > 250 definierten Alarmregeln

(Energieautomatisierungs- und SCADA-domänenspezifisch)

SIEM Regeln identifizieren „abnormales“ Verhalten.

Beispiele:

Mehrfach fehlgeschlagene Anmeldungen:
Mehrfach fehlgeschlagene Anmeldungen sind ein Hinweis auf unberechtigte Zugriffsversuche und sollten daher untersucht werden. Alarm bei >= 3 fehlgeschlagenen Logins innerhalb von fünf Minuten auf dem System mit einem Benutzernamen.

Zugriff auf nicht erlaubte IP Adresse:
Die Kommunikation im System ist klar definiert. Kommunikationsversuche mit IP Adressen außerhalb des Systems lösen einen Alarm aus.

Konfigurationsänderung eines OT-Gerätes:
Konfigurationsänderungen an OT-Geräten sind nur während der Wartungszeiten zulässig. Wenn dieser Alarm auftritt, prüfen Sie den Einsatzplan, ob die Konfigurationsänderung zulässig war.

■ ■ ■

SIEMENS

erweiterte Security Features in OT-Komponenten

Intrusion Detection & SYSLOG Funktionalitäten SICAM A8000

Erweiterte Funktionen zur Erkennung und Erfassung, sowie zur Analyse von Angriffen

Security Logbook

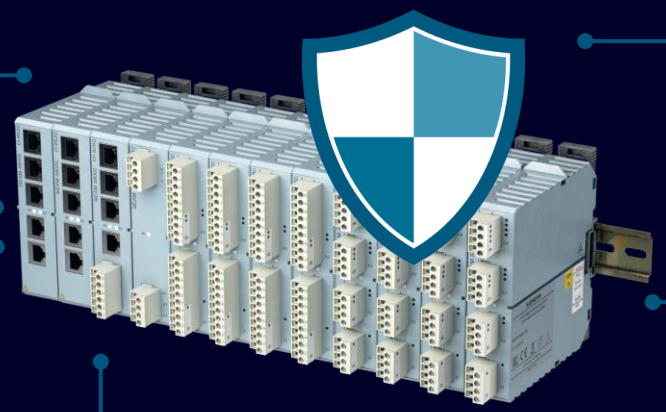
Spannungsausfallsichere Speicherung von (SRE) Ereignissen

LOG-Speicher Überlaufschutz

Schützt erweiterte Erfassungs-Funktionen, die den LOG-Speicher vor einem Überlauf und „False-Positives“ schützen

SYSLOG-Prozessinformationen

Erfassen und Weiterleiten von security-relevanten Prozessinformationen per SYSLOG ⇨ z.B. Türkontakt



SYSLOG-Kommunikationsinformationen

Erkennen und Erfassen von geblocktem Verkehr z.B. im White-List Filter (IEC -104 TI Verkehr)

ARP Spoofing

Erkennen und Erfassen von ARP Angriffen
https://de.wikipedia.org/wiki/ARP-Spoofing

SYN-Flood

Erkennen und Erfassen von TCP DoS SYN-Flood Angriffen
https://de.wikipedia.org/wiki/SYN-Flood

ARP = Address Resolution Protocol

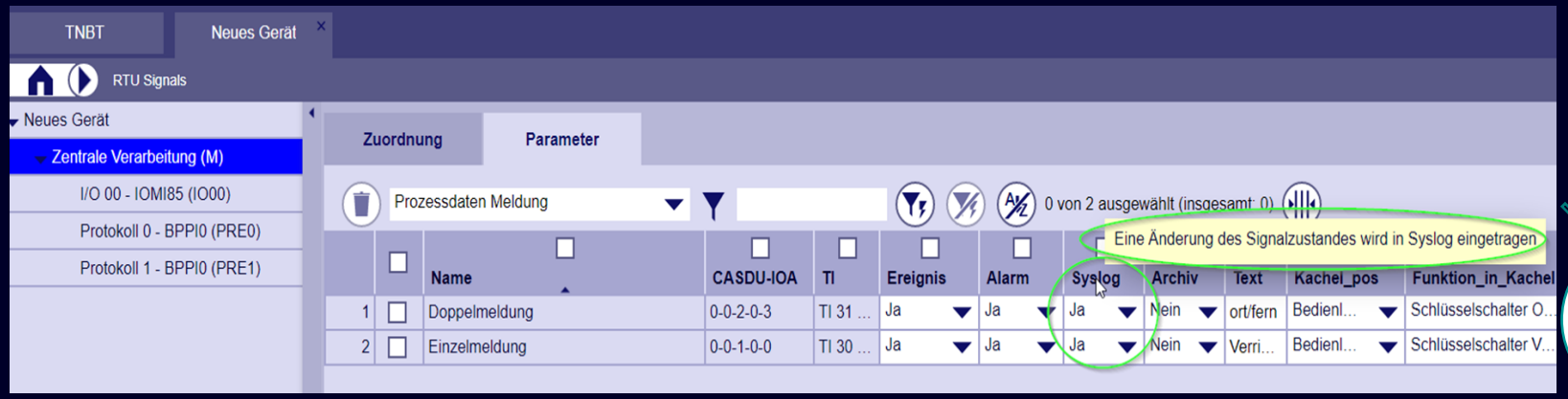
DoS = Denial of Service

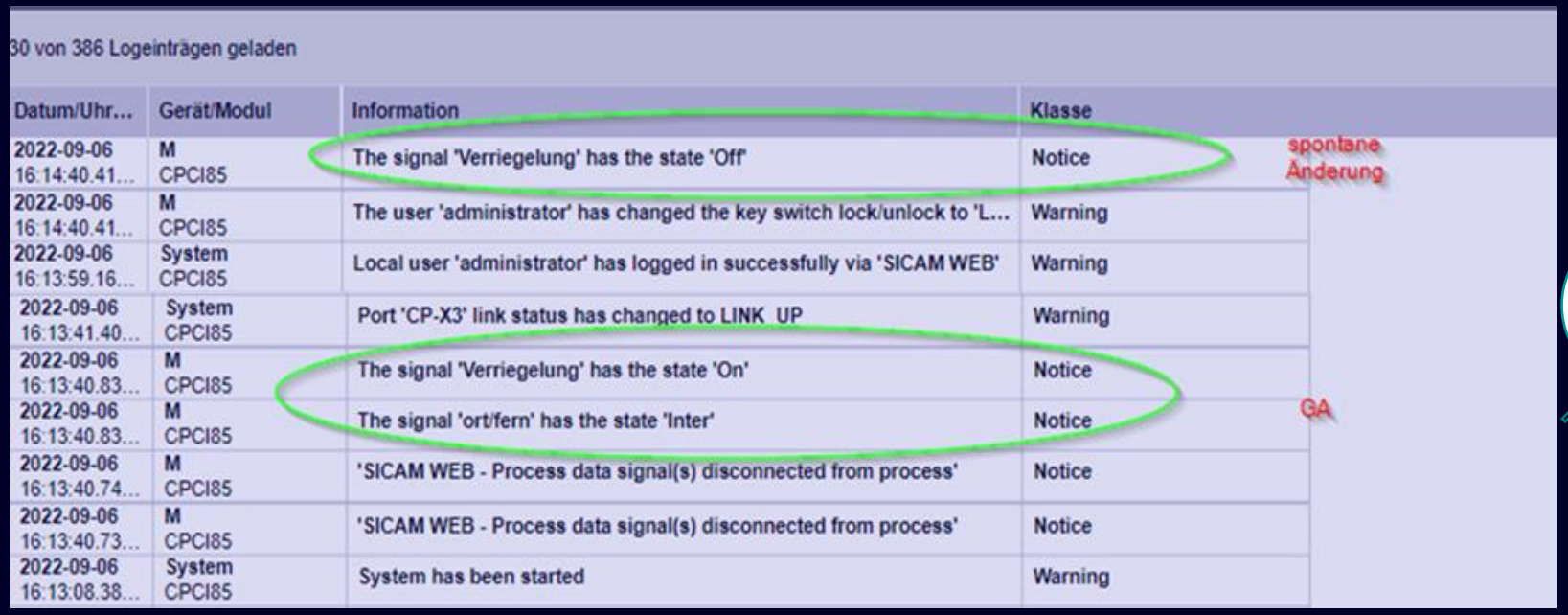
TCP Transmission Control Protocol

SIEMENS

Intrusion Detection / EDR Funktionalitäten

Prozessinformationen ⇨ SysLog



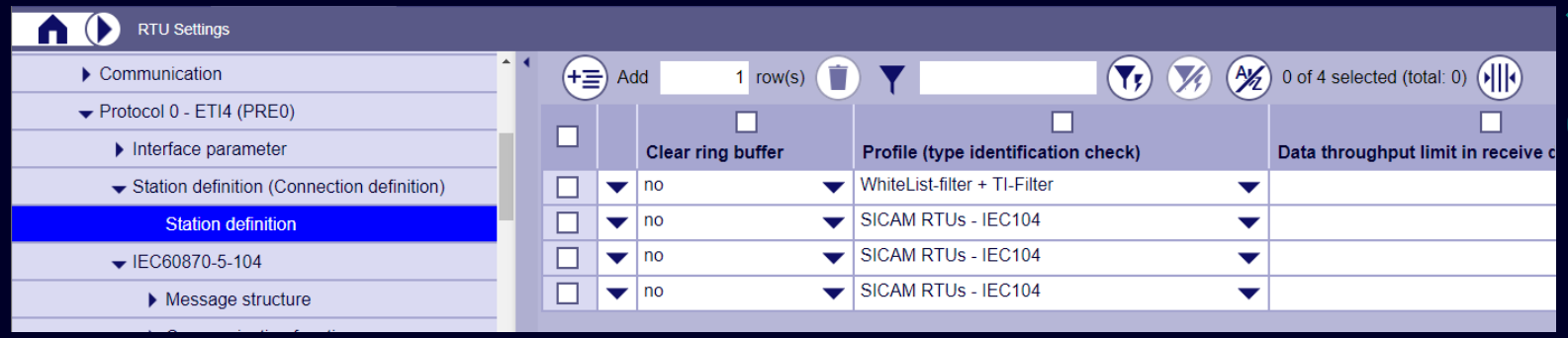


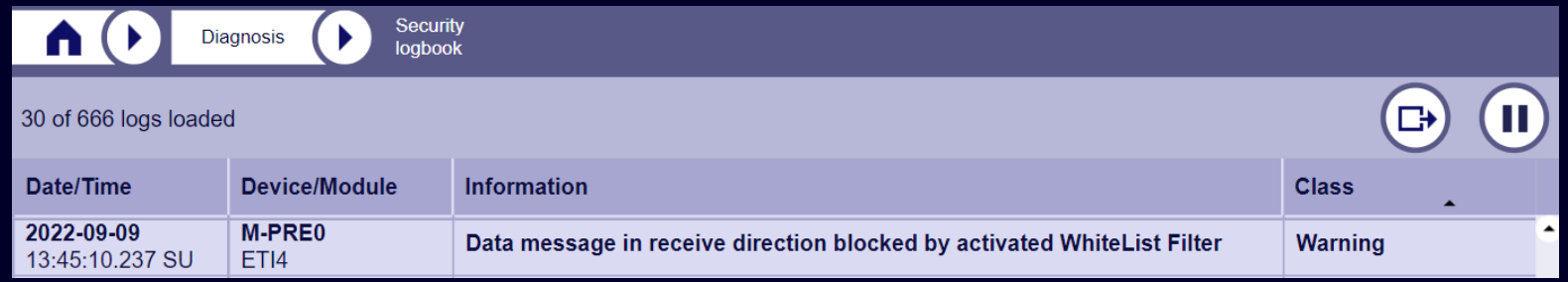
- Prozess-Daten z.B. Türkontakt
- Konfiguration wie andere Anwendungen
- Speicherung von Daten & Status im SYSLOG Speicher

SIEMENS

Intrusion Detection / EDR Funktionalitäten

Kommunikationsfinformationen: Verbesserungen TI / Whitelist-Filter 101 / 104



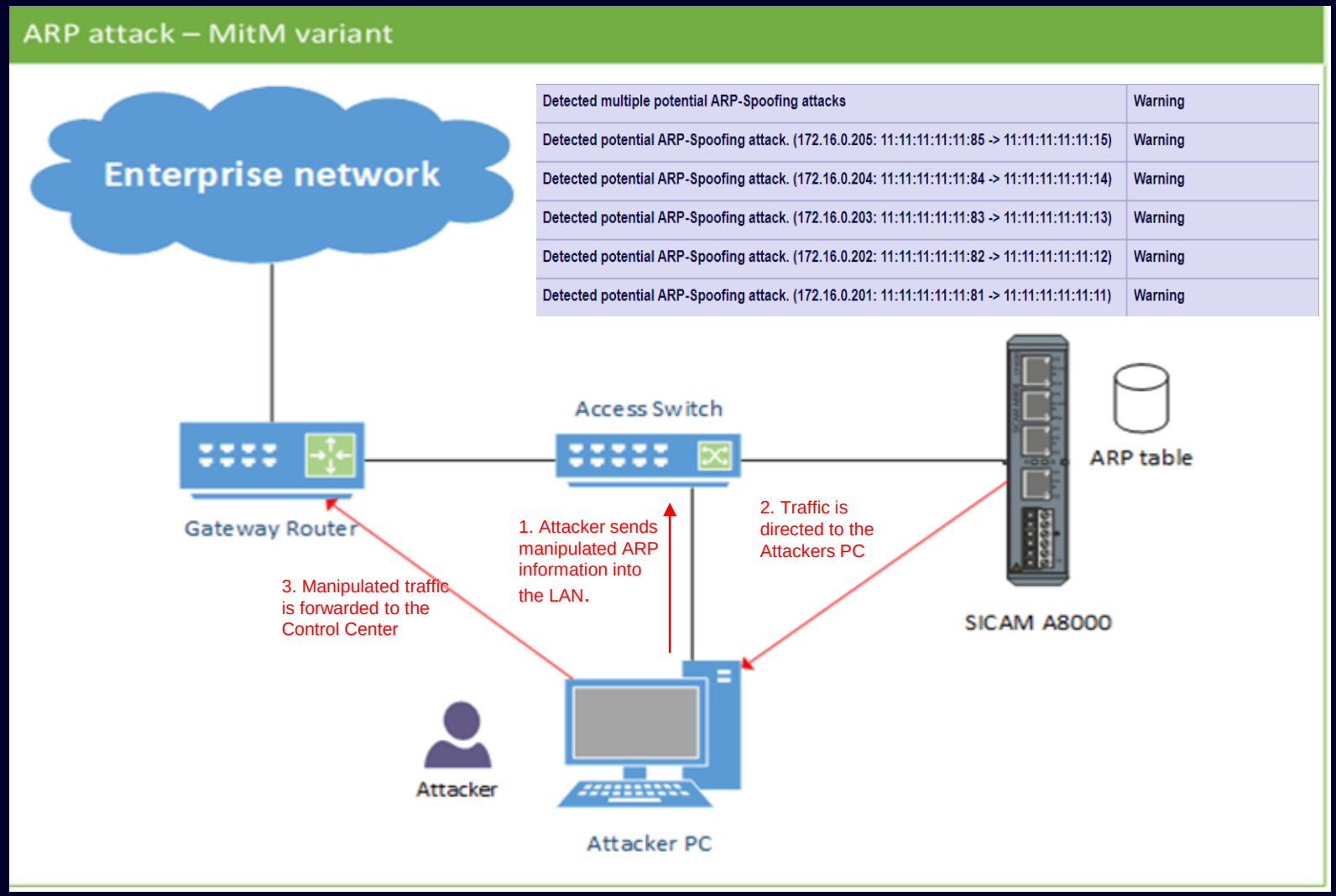


- Blockierte Typ Identifikation (TI) / Whitelist – Filter
- Syslog for IP / 104 Adresse
- Syslog maximales Erfassungs-Interval
- Syslog Erfassungs-Neustart

SIEMENS

zusätzliche IDS/EDR Funktionen (I)

Erkennung von Address Resolution Protocol (ARP) Angriffen



- Erkennung und Erfassung von ARP spoofing (ARP Manipulation)
- Schwellwert für die Angriffserkennung
- Syslog maximales Erfassungs-Interval
- Syslog Erfassungs-Neustart

ARP Address Resolution Protocol
dient der Zuordung von physikalischen (MAC) Adressen zu IP-Adressen

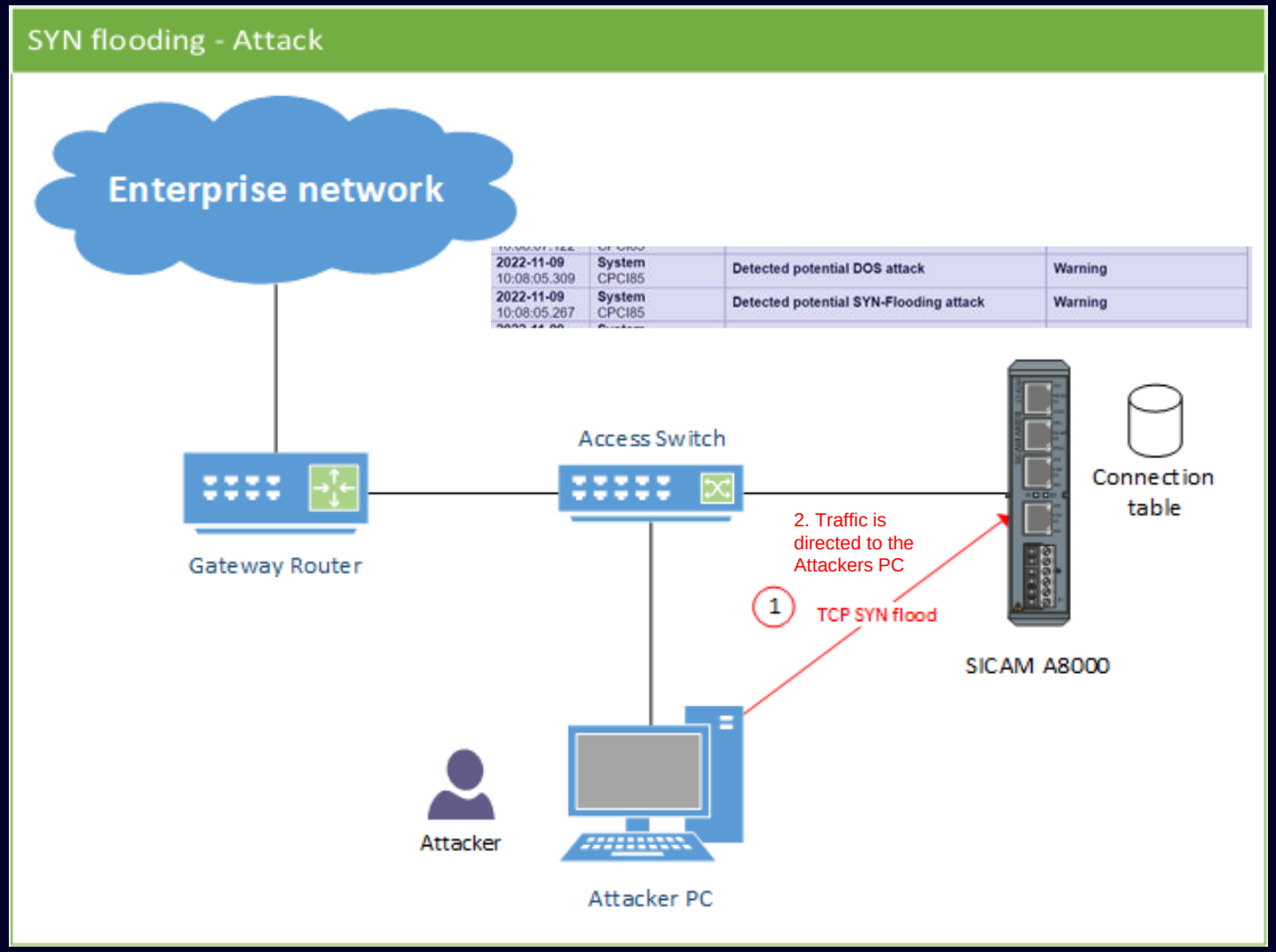
ARP spoofing manipuliert diese Zurodnung und leitet Verkehr zu einem Angreifer um

https://de.wikipedia.org/wiki/ARP-Spoofing

SIEMENS

zusätzliche IDS/EDR Funktionen (II)

Erkennung von SYN-Flood (DoS) Angriffen



- TCP SYN Flooding
- Allgemein bekannt als (D)DoS-Angriff
- Schwellwert: z.B. 2.000/Sekunde
- Syslog Erfassungs-Neustart

TCP SYNC Flooding:
Massenhaftes Senden von SYNC-Nachrichten, um TCP-Verbindungen aufzubauen und das Empfangssystem in Überlast zu bringen. Dies wird als DoS (Denial of Service) Angriff bezeichnert

https://de.wikipedia.org/wiki/SYN-Flood

SIEMENS

Kontakt

Herausgegeben von Siemens 2023

Georg Artmeier

RC-DE SI EA S PROM GA
Robert-Koch-Str. 5
82152 Planegg, Deutschland

Mobile:
+49 (0) 176 11728143

E-mail:
georg.artmeier@siemens.com

SIEMENS